# Commentaires sur l'agrégation interne 2007, comp. 1

Du vécu ? Des réactions ? Ces colonnes vous sont ouvertes !

## Je retrouve des passages bien connus !

(Dany-Jack Mercier, 3 jours après les épreuves,

soit le samedi 3 février 2007)

J'ai été très content de devoir corriger cette première partie de l'agrégation interne 2007 (1ère comp.) car... je l'avais déjà traitée dans mon volume III sur l'épreuve d'exposé au CAPES mathématique ! C'est cool, et cela m'a permis de retrouver les « passages cruciaux» plus rapidement... La Section 2.3.2 de mon « volume III » est entièrement dévolue à l'étude des triplets pythagoriciens, et le Théorème 32 ***contient exactement la démonstration demandée dans la question I.3.c*** utilisant $U=u^2$ et $V=v^2$. Celle-ci vient d'autant plus facilement à l'esprit qu'on l'a déjà rencontrée durant les années de préparation au concours. Lorsqu'on travaille le cours, il n'est donc pas inutile de travailler aussi les démonstrations des Théorèmes que l'on rencontre. La Section 17.3 placée en annexe du « volume III » (je vous le dis : ces annexes peuvent servir :) propose aussi trois problèmes sur les anneaux et l'arithmétique qui permettent de se préparer convenablement à ce type d'épreuve... et à la partie II de notre problème d'agrégation interne qui traite de l'anneau **Z**[iV2]. Cela me convainc de continuer à placer des annexes « tous azimuths » à la fin de mes bouquins.

Dernier point : il est essentiel d'éviter ces méprises graves concernant le « travail sur les entiers relatifs et la divisibilité ». Dire que « si d divise ab, alors d divise a ou d divise b » est super mortel, et ne pardonne ni à l'écrit, ni à l'oral. Il FAUT savoir (et savoir démontrer) que cette propriété caractérise les nombres premiers. Si l'erreur est faite à l'oral, elle est éliminatoire car le jury concluera que l'arithmétique n'a pas été travaillée par le candidat, et qu'une erreur aussi « énorme » n'a pas lieu d'être. On peut la faire par étourderie, mais il faudra se remettre sur les bons rails dès que le jury pose une question. On peut « se rattraper » après une étourderie, mais on ne peut pas s'en sortir si on persiste et montre que l'on a jamais réfléchi sur la leçon concernant les nombres premiers...

***Où l'écrit rejoint l'oral (et réciproquement) :*** on prépare toujours les deux en même temps, et la préparation de l'un sert de tremplin pour une bonne préparation de l'autre. C'est ce que j'aime à répéter... Bref, avant d'attaquer ce sujet d'agrégation interne 2007, je recommande de travailler les leçons d'oral sur les nombres premiers, sur l'anneau **Z**, et celle sur les pgcd. Ces leçons préparent réellement à cette épreuve (dans ma série

## Définition d'un irréductible

(Sami, 28 février 2007)

J'ai une question à vous poser qui me trotte dans la tête depuis...que je

composais ! Cela concerne la formulation de l'énoncé de l'épreuve 1, et donc de l'épreuve en elle-même : on définit un élément irréductible 'a' s'il vérifie la propriété suivante : "a=bc implique b inversible et/ou c inversible".

Considérons un élément 'd' inversible de Z[iV2]; si on écrit d sous la forme d=u.v avec u et v dans Z[iV2], les éléments inversibles de Z[iV2] étant ceux de norme 1, on a alors N(d)=1=N(u).N(v)...donc N(u)=N(v)=1 car N(u) et N(v) sont dans N. Ceci devient évidemment faux si on se plonge dans le corps des fractions Q[iV2] de Z[iV2], car dans ce cas, on a seulement u et v non nuls...

Ainsi, dans Z[iV2], tout élément inversible est irréductible, non ? J'aime l'arithmétique et pourtant, je ne m'étais jamais posé cette question sauf devant ma copie où la définition donnée d'un élément irréductible me paraissait un peu en contradiction avec la formulation d'une partie de l'épreuve. (...)

djm : Je vois... Il faut bien se rappeler, dès le départ, qu'un élément d'un anneau intègre A, est dit irréductible si et seulement si les 3 cpnditions suivantes sont vérifiées :

1) Il n'est pas nul,

2) Il n'est pas inversible (c'est ce qui vous tracasse),

3) a=bc implique b inversible ou c inversible.

L'énoncé ne comporte donc pas d'erreur car on précise "Soit alpha un élément non nul, et non inversible deA ; on dit que...". Ouf : heureusement que c'était marqué en début de phrase. Je pense que cela répond à votre question.

Un dernier point : dans un qcm d'un concours pour les impôts, il y a quelque temps, quelqu'un m'avait rapporté la question suivante : "1 est-il un nombre premier ?"

Diable, question pernicieuse s'il en est, car c'est bien par définition, et par commodité a posteriori, que l'on choisit de dire que 1 n'est pas un nombre premier. C'est un peu dégoutant pour notre pauvre "1" qui a le mérite de ne

## Le retour du pgcd(0,0)...

(Julien, 26 mai 2007)

Ma difficulté est la suivante et m'a gêné tout au long du devoir, pour être sûr que ce dont je parlais était bien défini, notamment à la partie V :

"Lorsqu'on considère un pgcd de plusieurs éléments d'un anneau, cela a-t-il un sens si certains de ces éléments sont nuls ?"

Je n'arrive pas à trancher étant donné que :

a) Etant défini (à inversible près) comme diviseur commun qui est multiple de tous les diviseurs communs, pgcd(0,0) n'existe pas dans Z (seule exception je crois), d'ailleurs je me souviens que mon prof d'Algèbre prenait bien soin de toujours se placer dans un anneau intègre A pour faire de l'arithmétique. Pourquoi faire sinon pour se réfugier dans la confortable partie A-{0}, stable du coup, et n'en plus sortir ?

b) D'un autre côté, il y a les définitions en d = pgcd(a,b) <=> aA + bA = dA. Alors là tout est possible et pgcd(0,0) = 0. Mais ceci ne concerne-t-il pas que les anneaux principaux ?

Une définition est libre, mais connaissez vous une définition officielle ? Si c'est la première que j'ai citée, je remarque que l'énoncé ne suppose pas alpha, beta, gamma non nuls dans la partie V.4. Et pourtant est posé n l'entier tq gamma soit encore multiple de $\pi^n$ et plus de $\pi^{n+1}$, ce qui n'aurait pas de sens si gamma était nul. Si un pgcd est bien défini comme je le pense (version 1), quelle erreur me semble-t-il que de ne s'être pas explicitement placé dans le cadre où il avait un sens en supposant alpha, beta, gamma non nuls.

Cette ambiguité rend pénible la rédaction de la conclusion à la question V.5), et mon embarras a dû être partagé par bien des candidats lorsqu'il s'est agi de relier la contradiction obtenue au fait qu'un des nombres x,y,z tel que x^3 + y^3 = z^3 était nécessairement nul.

C'est pourquoi je voulais vous demander des précisions au sujet de la définition d'un pgcd, (et même de l'énoncé V.4.) et plus généralement sur la nécessité de se supposer intègres les anneaux dans lesquels on se place.

djm : Une première remarque au sujet du problème. Dans la partie I, on travaille dans **Z**

« L'épreuve d'exposé au CAPES » : Volume I, Ch. 5 ; Volume II, Ch. 1 et 2 ; et Volume III Ch. 1 et 2).

posséder QUE des diviseurs triviaux. Or, il est agréable (et c'est presque ce que l'on fait) de dire qu'un entier relatif est premier si et seulement si il ne possède que des diviseurs triviaux. On doit rajouter "un entier relatif non nul et distinct de 1 et -1"... Un nombre premier p possède donc exactement 4 diviseurs triviaux 1, -1, p, -p. Hum... c'est méchant en qcm pour les impôts, et un tantinet injuste, puisqu'une définition n'est posée que "par commodité" et dans le but de faciliter les énoncés qui suivent, non ? (...)

ou dans **N**. Dans toutes les autres parties III à V, on se place souvent dans deux autres anneaux, mais on prend soin de démontrer qu'il s'agit d'anneaux principaux. La définition d'un pgcd de deux éléments d'un anneau principal étant connue, par exemple en écrivant si justement aA + bA = dA comme vous le faites, il n'y a pas de problème dans ce problème !

Il va sans dire que j'utilise cette belle écriture aA + bA = dA pour définir « un » pgcd d de a et b ; et que, par conséquent, un pgcd de 0 et 0 est 0.

Restons dans un anneau principal. Dans un tel anneau, on sait que définir d par aA + bA = dA équivaut à dire que d vérifie : « x divise d ssi x divise simultanément a et b » (voir par exemple le document suivant sur MégaMaths concernant les anneaux principaux, le Théorème 2 plus précisément). Comme il est vrai que « x divise 0 ssi x divise simultanément 0 et 0 », on peut aussi dire que 0=pgcd(0,0). Et heureusement.

Le seul problème qu'il y aurait à choisir pgcd(0,0)=0, et que cela ne correspond plus à la « très bonne image » du pgcd que nous nous faisons, en voyant ce nombre comme le plus grand diviseur commun de a et b, au sens de notre bonne vieille relation d'ordre <=. C'est peut-être la relation d'ordre qu'il faut changer ! Car si 0 n'est pas le plus grand diviseur de 0 et de 0 au sens de la relation <= (il n'en existe pas en fait pour cette relation... car tout nombre divise 0. Ou alors il faudrait poser pgcd(0,0)=+oo...), 0 demeure le plus grand diviseur de 0 et 0 dans l'ensemble **N** des entiers naturels muni de la relation d'ordre « divise ». Voilà la relation d'ordre adaptée à la pratique du pgcd de 0 et 0 :)))

En fait, on pourrait dire que tout va bien aussi dans Z, mais il y a juste un petit problème : la relation divise n'est alors qu'une relation de préordre... Mais ce n'est pas gênant si on « généralise » en quelque sorte la notion de « plus grand élément » d'une partie d'un ensemble ordonnée pour en parler encore (sans l'unicité) lorsque la partie est celle d'un ensemble muni d'un simple préordre.

Voilà des pistes de réponse... Pour aller plus loin, on pourra regarder la Section 1.2.6 de mon livre « L'épreuve d'exposé au CAPES math., vol. III » qui s'intitule « Sur une question du jury posée en juin 2004 » et en plein dans le sujet ! Le jury ayant posé une question sur la convention (éventuelleà suivant laquelle pgcd(0,0)=0.

Dans N, le pgcd de deux éléments existe car on peut parler de « treillis », on dit aussi « ensemble réticulé », c'est-à-dire d'un ensemble ordonné dans lequel toute partie à deux éléments admet une borne supérieure et une borne inférieure. C'est tout N muni de la relation « divise »...

Pour terminer, je noterai que l'on peut parler de pgcd et de ppcm dans n'importe quel anneau intègre (ça, c'est important sinon on part dans le décors), mais que dans ce cas, il se peut que deux élément n'aient pas de pgcd ou de ppcm... Car la définition est alors la suivante : si la famille d'idéaux principaux {aA, bA} admet une borne inférieure dA dans l'ensemble P des idéaux principaux de A, alors d est appelé « un pgcd de a et b ». Une telle définition ne mange pas de pain... et n'affirme aucune existence. Et l'on a encore aA + bA = dA, i.e. « x divise d ssi x divise simultanément a et b », la seule différence est que ce joli élément d n'existe pas forcément.

On notera que parler d'idéaus nous permet d'utiliser la relation d'ordre « inclusion » qui a le bon goût de représenter la relation « divise » qui n'est qu'un préordre... et de nous permettre de parler de borne inférieure (de façon juste et mesurée :), donc de plus grand élément de l'ensemble des minorants de la partie {aA, bA}.

Bien entendu, si A est principal, deux éléments quelconques auront toujours des pgcd... C'est bien ce qui est extraordinaire, et qu'on ne se prive pas d'utiliser.

Rajoutons que lorsque A est factoriel, deux éléments quelconques ont encore toujours un pgcd... Comment l'obtient-on ?

Finalement toutes ces définitions ne font qu'un, et il est naturel de poser pgcd(0,0)=0.